What is claimed is:

1. A method of monitoring traffic flow in a monitor device disposed to receive network traffic packets comprises:

producing statistics corresponding to a parameter of traffic flow to trace the source of an attack, with producing further comprising:

mapping the traffic flow into a plurality of buckets by applying a hash function "f(h)" to the parameter of the traffic flow to output an integer corresponding to one of the buckets;

accumulating statistics from the packets; and

comparing the number of buckets to a threshold; and

determining whether the number of buckets should be divided into more buckets or combined into fewer buckets based on comparing the number of buckets to the threshold.

2. The method of claim 1 wherein the buckets are storage areas in a memory space of the monitor device.

3. The method of claim 1 wherein as the number of buckets changes, the buckets have values derived from the buckets prior to the change.

4. The method of claim 1 wherein the hash function adapts to map to the new number of buckets, as the new number of buckets changes.

5. The method of claim 1 wherein comparing statistic values comprises:

comparing the value accumulated in the bucket to a threshold that depends on the number of buckets.

6. The method of claim 1 wherein the parameter is the count of how many packets a data collector or gateway examines.

7. The method of claim 1 wherein as a value of a parameter for one bucket approaches a threshold, the monitoring device raises an alarm.

8. The method of claim 1 wherein the hash function changes periodically in a randomly secret manner so that packets are reassigned to different buckets.

9. The method of claim 1 wherein the variable number of buckets dynamically adjusts the amount of traffic and number of flows monitored, so that the monitoring device is not vulnerable to a denial of service attack against its own resources.

10. The method of claim 1 wherein the variable number of buckets efficiently identifies the source or sources of attack by breaking down traffic into different buckets and examining statistics accumulated for a parameter and a corresponding threshold in each bucket.

11. The method of claim 1 wherein the traffic is monitored at multiple levels of granularity, from aggregate to individual flows.

12. The method of claim 1 wherein the traffic is applied to monitoring of TCP packet ratios and repressor traffic.

13. The method of claim 1 wherein the threshold is a first threshold and the method further comprises:

comparing accumulated statistic values from the buckets to second threshold values to determine that an event is of significance.

14. A computer program product residing on a computer readable for monitoring network traffic flow in a network comprises instructions for causing a computer to:

map traffic flow into a plurality of buckets by applying a hash function "f(h)" to a parameter of the traffic flow to output an integer corresponding to one of the buckets;

accumulate statistics from the packets; and

compare the accumulated statistic values from the buckets to configured threshold values corresponding to the number of buckets to determine that an event is of significance; and

adjust the number of buckets as the number of buckets approaches a second threshold.

15. The computer program product of claim 14 wherein based on the second threshold, the buckets are divided into more buckets or combined into fewer buckets

16. The computer program product of claim 14 wherein instructions to monitor further comprise instructions to

divide the bucket into a different number of new buckets containing values derived from the original bucket.

17. The computer program product of claim 14 wherein the hash function adapts to map to the new number of buckets as the new number of buckets changes.

18. The computer program product of claim 14 wherein the parameter is the count of how many packets a data collector or gateway examines.

19. The computer program product of claim 14 wherein the buckets are storage areas in the memory space of the monitor device.

20. The computer program product of claim 14 wherein the hash function changes periodically in a randomly secret manner so that packets are reassigned to different buckets.

21. A data collector to collect statistical information about network flows comprises:

a computer readable medium;

a computing device that executes a computer program product stored on the computer readable medium comprising instructions to cause the computing device to:

map traffic flow into a plurality of buckets by applying a hash function "f(h)" to the parameter of the traffic flow to output an integer corresponding to one of the buckets;

accumulate statistics from the packets; and

compare the accumulated statistic values from the buckets to configured threshold values corresponding to the number of buckets to determine that an event is of significance; and

adjust the number of buckets as the number of buckets approaches a second threshold; and

a port to link the data collector to a central control center.

22. A method of detecting a denial of service attack on a victim site, the method comprising:

monitoring network traffic sent to the victim site;

determining a ratio of incoming to outgoing TCP packets destined and sourced from systems at the site;

comparing the ratio to a threshold value; and

raising an alarm when the ratio exceeds the threshold value.

23. The method of claim 22 wherein monitoring further comprises:

storing the determined ratio over periods of time; and

analyzing the ratio to determine over time how much and how the ratio exceeds a value to set a threshold.

24. The method of claim 22 wherein monitoring further comprises:

establishing the ratio, and as the ratio exceeds that established threshold raising the alarm.

25. The method of claim 22 wherein the ratio is about 2:1 for incoming to outgoing TCP packets.

26. The method of claim 22 wherein as the ratio exceeds the threshold it is a indication that the victim is receiving bad TCP traffic that are not part of any established TCP connection.

27. The method of claim 22 wherein as the ratio exceeds the threshold, exceeding the threshold raises an indication that the victim is overloaded to acknowledge the requests.

28. The method of claim 22 wherein monitoring comprises:

producing statistics corresponding to the ratio by mapping the traffic flow into a plurality of buckets by applying a hash function "f(h)" to the parameter of the traffic flow to output an integer corresponding to one of the buckets.

29. The method of claim 28 further comprises:

communicating the statistics collected to a control center.

30. The method of claim 29 wherein communicating occurs over a dedicated link to the control center via a hardened network.

31. The method of claim 30 executed on a gateway physically deployed in the network.

32. A monitor device to collect statistical information about network flows comprises:

a computer readable medium;

a computing device that executes a computer program product stored on the computer readable medium comprising instructions to cause the computing device to:

monitor network traffic sent to the victim site;

determine a ratio of incoming to outgoing TCP packets destined and sourced from systems at the site;

compare the ratio to a threshold value; and

raise an alarm when the ratio exceeds the threshold value.

33. The monitor device of claim 32 wherein the monitor is a gateway.

34. The monitor device of claim 32 wherein wherein the ratio is about 2:1 for incoming to outgoing TCP packets.

35. A method of detecting a denial of service attack on a victim site, the method comprising:

monitoring network traffic sent to the victim site;

determining a ratio of incoming to outgoing TCP packets destined and sourced from systems at the site;

comparing the ratio to a threshold value; and

raising an alarm when the ratio exceeds the threshold value.

36. The method of claim 35 wherein monitoring further comprises:

storing the determined ratio over periods of time; and

analyzing the ratio to determine over time how much and how the ratio exceeds a value to set a threshold.

37. The method of claim 35 wherein monitoring further comprises:

establishing the ratio and as the ratio exceeds that threshold raising the alarm.

38. The method of claim 35 wherein the ratio is about 2:1, for incoming to outgoing TCP packets.

39. The method of claim 35 wherein the ratio is up to about 3:1, for incoming to outgoing TCP packets.

40. The method of claim 35 wherein as the ratio exceeds the threshold it is a indication that the victim is receiving bad TCP traffic that are not part of any established TCP connection.

41. The method of claim 35 wherein monitoring comprises:

producing statistics corresponding to the ratio by mapping the traffic flow into a plurality of buckets by applying a hash function "f(h)" to source addresses of the traffic flow to output an integer corresponding to one of the buckets.

42. The method of claim 41 further comprises:

communicating the statistics collected to a control center.

43. The method of claim 42 wherein communicating occurs over a dedicated link to the control center via a hardened network.

44. The method of claim 43 executed on a gateway physically deployed in the network.

45. A method of detecting a denial of service attack on a victim site, the method comprising:

monitoring network traffic sent to the victim site and identify packets generated from repressor traffic;

analyzing message header information from identified packets; and

generating logs of contents of the message headers guard against attackes.

46. The method of claim 45 wherein the logs are generated for forensic purposes or to selectively block future messages similar to the ones that caused the repressor traffic messages.

47. The method of claim 45 wherein the repressor traffic is ICMP port unreachable messages that are generated by an end host when it receives a packet on a port that is not responding to requests.

48. The method of claim 45 wherein repressor traffic is any network traffic that is indicative of problems or a potential attack in a main flow of traffic.

49. The method of claim 45 wherein the method is executed on a gateway.